TO: USPTO

ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	October 20, 2006	**Phone Number**	**Fax Number**
To:	Board of Patent Appeals, USPTO		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P449/01.143.01 **App. No: 09/976,009**

Total Number of Pages Being Transmitted, Including Cover Sheet: 38

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

October 20, 2006

RECEIVED
CENTRAL FAX CENTER
OCT 2 0 2006

Practitioner's Docket No. NAI1P449/01.143.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Neil John Hursey et al.

Application No.: 09/976,009 Group No.: 2136
Filed: 10/15/2001 Examiner: Colin, Carl G.
For: UPDATING MALWARE DEFINITION DATA FOR MOBILE DATA PROCESSING DEVICES

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION–37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application. This brief is in furtherance of the Notice of Appeal, filed in this case on 05/23/2006, and the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 07/20/06.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*

(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Date: 10/20/2006

Erica L. Farlow

Signature

Erica L. Farlow

(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for two months:

Fee:	$450.00

If an additional extension of time is required, please consider this a petition therefor.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$450.00
TOTAL FEE DUE	**$950.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $950.00 to Deposit Account No. 50-1351 (Order No. NAI1P449).

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P449).

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Hursey et al.	Group Art Unit: 2136
Application No. 09/976,009	Examiner: Colin, Carl G.
Filed: 10/15/2001	Date: 10/20/2006
For: UPDATING MALWARE DEFINITION DATA FOR MOBILE DATA PROCESSING DEVICES	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 05/23/2006, and the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 07/20/06.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-3, 5-12, 14-21, 23-30, 32-39, 41-48, and 50-54

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-3, 5-12, 14-21, 23-30, 32-39, 41-48, and 50-54
3. Claims allowed: None
4. Claims rejected: 1-3, 5-12, 14-21, 23-30, 32-39, 41-48, and 50-54
5. Claims cancelled: 4, 13, 22, 31, 40, and 49

C. CLAIMS ON APPEAL

The claims on appeal are: 1-3, 5-12, 14-21, 23-30, 32-39, 41-48, and 50-54

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1-4, a computer program product embodied on a computer readable medium is provided for controlling a mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.) to update malware definition data for a malware scanner of the mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.). In use, a wireless telephony link is established between the mobile data processing device and a public wireless telephony network. Further, malware definition updating data is received at the mobile data processing device via a data channel of the wireless telephony link (e.g. see items 36 and 38 of Figure 3, etc.). In addition, malware definition data (e.g. see item 34 of Figure 2, etc.) stored upon the mobile data processing device is updated using the malware definition updating data. The mobile data processing device registers with a base station (e.g. see items 4 and 10 of Figure 1, etc.) of the wireless telephony network when the link is established such that the base station and the wireless telephony network are notified of a telephone number of the mobile data processing device for use in sending the malware definition updating data to the mobile data processing device. Also, when data is received at the mobile data processing device, a type of the received data is identified (e.g. see item 38 of Figure 3, etc.) to determine if the received data is the malware definition updating data. If the received data is the malware definition updating data, a digital signature associated with the malware definition updating data is verified (e.g. see item 42 of Figure 3, etc.). If the digital signature is not verified, the malware definition updating data is ignored. Also, if the digital signature is verified, the malware definition updating data is utilized to update the malware definition data stored upon the mobile data processing device by appending the malware definition updating data to the malware definition data (e.g. see item 44 of Figure 3, etc.). The malware definition updating data is provided in a malware definition updating file. The file is generated automatically, semi-automatically, or manually upon an analysis of newly discovered malware, and the file includes a detection fingerprint and either a removal action or a disinfection action to be taken in response to a detection of the newly discovered malware. In addition, the mobile data processing device is identified by a database of subscribers to an update service associated with the malware scanner (e.g. see item 50 of Figure 4, etc.). The database includes the telephone number of the mobile data processing device to which the malware definition updating data is to be sent and a type of the mobile data processing

device such that only malware definition updating data that is appropriate to the type of the mobile data processing device is sent to the mobile data processing device. See, for example, page 3, lines 6-17; page 8, lines 1-11; page 8, lines 13-27; page 8, line 29 – page 9, line 2; page 9, lines 4-9; and page 9, lines 14-20 et al.

With respect to a summary of Claim 10, as shown in Figures 1-4, a computer program product embodied on a computer readable medium is provided for controlling a computer to initiate updating of malware definition data (e.g. see item 34 of Figure 2, etc.) for a malware scanner of a mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.). In use, a wireless telephony link is established between the mobile data processing device via a public wireless telephony network. Further, malware definition updating data is sent (e.g. see item 50 Figure 4, etc.) to said mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.) via a data channel of said wireless telephony link. The mobile data processing device registers with a base station (e.g. see items 4 and 10 of Figure 1, etc.) of the wireless telephony network when the link is established such that the base station and the wireless telephony network are notified of a telephone number of the mobile data processing device for use in sending the malware definition updating data to the mobile data processing device. Also, when data is received at the mobile data processing device, a type of the received data is identified (e.g. see item 38 of Figure 3, etc.) to determine if the received data is the malware definition updating data. If the received data is the malware definition updating data, a digital signature associated with the malware definition updating data is verified (e.g. see item 42 of Figure 3, etc.). If the digital signature is not verified, the malware definition updating data is ignored. Also, if the digital signature is verified, the malware definition updating data is utilized to update the malware definition data stored upon the mobile data processing device by appending the malware definition updating data to the malware definition data (e.g. see item 44 of Figure 3, etc.). The malware definition updating data is provided in a malware definition updating file. The file is generated automatically, semi-automatically, or manually upon an analysis of newly discovered malware and, the file includes a detection fingerprint and either a removal action or a disinfection action to be taken in response to a detection of the newly discovered malware. In addition, the mobile data processing device is identified by a database of subscribers to an update service associated with the malware scanner (e.g. see item 50 of Figure 4, etc.). The database includes the telephone number of the mobile data processing device to which the malware definition updating

data is to be sent and a type of the mobile data processing device such that only malware definition updating data that is appropriate to the type of the mobile data processing device is sent to the mobile data processing device. See, for example, page 8, lines 1-11; page 8, lines 13-27; page 8, line 29 – page 9, line 2; and page 9, lines 4-20; et al.

With respect to a summary of Claim 19, as shown in Figures 1-4, a method is provided for updating malware definition data for a malware scanner of a mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.). In use, a wireless telephony link is established between the mobile data processing device and a public wireless telephony network. Further, malware definition updating data is received at the mobile data processing device via a data channel of the wireless telephony link. In addition, malware definition data (e.g. see item 34 of Figure 2, etc.) stored upon the mobile data processing device is updated using the malware definition updating data. The mobile data processing device registers with a base station (e.g. see items 4 and 10 of Figure 1, etc.) of the wireless telephony network when the link is established such that the base station and the wireless telephony network are notified of a telephone number of the mobile data processing device for use in sending the malware definition updating data to the mobile data processing device. Also, when data is received at the mobile data processing device, a type of the received data is identified (e.g. see item 38 of Figure 3, etc.) to determine if the received data is the malware definition updating data. If the received data is the malware definition updating data, a digital signature associated with the malware definition updating data is verified (e.g. see item 42 of Figure 3, etc.). If the digital signature is not verified, the malware definition updating data is ignored. Also, if the digital signature is verified, the malware definition updating data is utilized to update the malware definition data stored upon the mobile data processing device by appending the malware definition updating data to the malware definition data (e.g. see item 44 of Figure 3, etc.). The malware definition updating data is provided in a malware definition updating file. The file is generated automatically, semi-automatically, or manually upon an analysis of newly discovered malware, and the file includes a detection fingerprint and either a removal action or a disinfection action to be taken in response to a detection of the newly discovered malware. In addition, the mobile data processing device is identified by a database of subscribers to an update service associated with the malware scanner (e.g. see item 50 of Figure 4, etc.). The database includes the telephone number of the mobile data processing device to which the malware definition updating data is to be sent and a type of the mobile data processing

device such that only malware definition updating data that is appropriate to the type of the mobile data processing device is sent to the mobile data processing device. See, for example, page 3, lines 6-17; page 8, lines 1-11; page 8, lines 13-27; page 8, line 29 – page 9, line 2; page 9, lines 4-9; and page 9, lines 14-20 et al.

With respect to a summary of Claim 28, as shown in Figures 1-4, a method is provided for updating malware definition data (e.g. see item 34 of Figure 2, etc.) for a malware scanner of a mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.). In use, a wireless telephony link is established between the mobile data processing device via a public wireless telephony network. Further, malware definition updating data is sent (e.g. see item 50 Figure 4, etc.) to said mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.) via a data channel of said wireless telephony link. The mobile data processing device registers with a base station (e.g. see items 4 and 10 of Figure 1, etc.) of the wireless telephony network when the link is established such that the base station and the wireless telephony network are notified of a telephone number of the mobile data processing device for use in sending the malware definition updating data to the mobile data processing device. Also, when data is received at the mobile data processing device, a type of the received data is identified (e.g. see item 38 of Figure 3, etc.) to determine if the received data is the malware definition updating data. If the received data is the malware definition updating data, a digital signature associated with the malware definition updating data is verified (e.g. see item 42 of Figure 3, etc.). If the digital signature is not verified, the malware definition updating data is ignored. Also, if the digital signature is verified, the malware definition updating data is utilized to update the malware definition data stored upon the mobile data processing device by appending the malware definition updating data to the malware definition data (e.g. see item 44 of Figure 3, etc.). The malware definition updating data is provided in a malware definition updating file. The file is generated automatically, semi-automatically, or manually upon an analysis of newly discovered malware and, the file includes a detection fingerprint and either a removal action or a disinfection action to be taken in response to a detection of the newly discovered malware. In addition, the mobile data processing device is identified by a database of subscribers to an update service associated with the malware scanner (e.g. see item 50 of Figure 4, etc.). The database includes the telephone number of the mobile data processing device to which the malware definition updating data is to be sent and a type of the mobile data processing device such that only malware

definition updating data that is appropriate to the type of the mobile data processing device is sent to the mobile data processing device. See, for example, page 8, lines 1-11; page 8, lines 13-27; page 8, line 29 – page 9, line 2; and page 9, lines 4-20; et al.

With respect to a summary of Claim 37, as shown in Figures 1-4, an apparatus is provided for controlling a mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.) to update malware definition data for a malware scanner of the mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.). In use, a wireless telephony link is established between the mobile data processing device and a public wireless telephony network. Further, malware definition updating data is received at the mobile data processing device via a data channel of the wireless telephony link. In addition, malware definition data (e.g. see item 34 of Figure 2, etc.) stored upon the mobile data processing device is updated using the malware definition updating data. The mobile data processing device registers with a base station (e.g. see items 4 and 10 of Figure 1, etc.) of the wireless telephony network when the link is established such that the base station and the wireless telephony network are notified of a telephone number of the mobile data processing device for use in sending the malware definition updating data to the mobile data processing device. Also, when data is received at the mobile data processing device, a type of the received data is identified (e.g. see item 38 of Figure 3, etc.) to determine if the received data is the malware definition updating data. If the received data is the malware definition updating data, a digital signature associated with the malware definition updating data is verified (e.g. see item 42 of Figure 3, etc.). If the digital signature is not verified, the malware definition updating data is ignored. Also, if the digital signature is verified, the malware definition updating data is utilized to update the malware definition data stored upon the mobile data processing device by appending the malware definition updating data to the malware definition data (e.g. see item 44 of Figure 3, etc.). The malware definition updating data is provided in a malware definition updating file. The file is generated automatically, semi-automatically, or manually upon an analysis of newly discovered malware, and the file includes a detection fingerprint and either a removal action or a disinfection action to be taken in response to a detection of the newly discovered malware. In addition, the mobile data processing device is identified by a database of subscribers to an update service associated with the malware scanner (e.g. see item 50 of Figure 4, etc.). The database includes the telephone number of the mobile data processing device to which the malware definition updating data is to be sent and a type of the mobile data processing

device such that only malware definition updating data that is appropriate to the type of the mobile data processing device is sent to the mobile data processing device. See, for example, page 3, lines 6-17; page 8, lines 1-11; page 8, lines 13-27; page 8, line 29 – page 9, line 2; page 9, lines 4-9; and page 9, lines 14-20 et al.

With respect to a summary of Claim 46, as shown in Figures 1-4, a computer program product embodied on a computer readable medium is provided for controlling a computer to initiate updating of malware definition data (e.g. see item 34 of Figure 2, etc.) for a malware scanner of a mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.). In use, a wireless telephony link is established between the mobile data processing device via a public wireless telephony network. Further, malware definition updating data is sent (e.g. see item 50 Figure 4, etc.) to said mobile data processing device (e.g. see items 2 and 6 of Figure 1, etc.) via a data channel of said wireless telephony link. The mobile data processing device registers with a base station (e.g. see items 4 and 10 of Figure 1, etc.) of the wireless telephony network when the link is established such that the base station and the wireless telephony network are notified of a telephone number of the mobile data processing device for use in sending the malware definition updating data to the mobile data processing device. Also, when data is received at the mobile data processing device, a type of the received data is identified (e.g. see item 38 of Figure 3, etc.) to determine if the received data is the malware definition updating data. If the received data is the malware definition updating data, a digital signature associated with the malware definition updating data is verified (e.g. see item 42 of Figure 3, etc.). If the digital signature is not verified, the malware definition updating data is ignored. Also, if the digital signature is verified, the malware definition updating data is utilized to update the malware definition data stored upon the mobile data processing device by appending the malware definition updating data to the malware definition data (e.g. see item 44 of Figure 3, etc.). The malware definition updating data is provided in a malware definition updating file. The file is generated automatically, semi-automatically, or manually upon an analysis of newly discovered malware and, the file includes a detection fingerprint and either a removal action or a disinfection action to be taken in response to a detection of the newly discovered malware. In addition, the mobile data processing device is identified by a database of subscribers to an update service associated with the malware scanner (e.g. see item 50 of Figure 4, etc.). The database includes the telephone number of the mobile data processing device to which the malware definition updating

data is to be sent and a type of the mobile data processing device such that only malware definition updating data that is appropriate to the type of the mobile data processing device is sent to the mobile data processing device. See, for example, page 8, lines 1-11; page 8, lines 13-27; page 8, line 29 – page 9, line 2; and page 9, lines 4-20; et al.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-3, 5-12, 14-21, 23-30, 32-39, 41-48 and 50-54 under 35 U.S.C. 103(a) as being unpatentable over Lahti et al. (U.S. Publication No. 2002/0042886) in view of Hansson (WO 98/38820).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-3, 5-12, 14-21, 23-30, 32-39, 41-48 and 50-54 under 35 U.S.C. 103(a) as being unpatentable over Lahti et al. (U.S. Publication No. 2002/0042886) in view of Hansson (WO 98/38820).

Group #1: Claims 1-3, 5-12, 14-21, 23-30, 32-39, 41-48 and 50-54

With respect to independent Claims 1, 10, 19, 28, 37, and 46, the Examiner has relied on paragraphs [0019] and [0023] in Lahti along with page 6, lines 1-5 in Hansson to make a prior art showing of appellant's claimed technique "wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device."

First, appellant respectfully asserts that neither Lahti nor Hansson disclose a "mobile data processing device [that] registers with a base station of said wireless telephony network when said link is established," as claimed by appellant (emphasis added). In particular, Lahti only generally teaches that "a record of all subscribers to the anti-virus server [is maintained] in a database" (paragraph [0023]), but not that a "mobile data processing device registers with a base station...when said link is established," as appellant claims. In addition, the entire Hansson reference, and in particular the excerpt in Hansson relied on by the Examiner, fails to even suggest any sort of registration, and especially not in the specific manner claimed by appellant.

Second, appellant notes that the Examiner has relied on Hansson's disclosure of an "update server processor 100 [that] downloads the software by placing a call to the cellular phone and

performing...[a] data transfer to the cellular telephone 110." Appellant respectfully asserts that simply utilizing a phone number to transfer a download does not meet appellant's specific claim language, namely that a "mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device" (emphasis added), in the context claimed.

In fact, appellant emphasizes that Hansson actually *teaches away* from registering such that notification of a telephone number is made, in the manner claimed by appellant, since Hansson discloses that "[i]n response to the cellular telephone subscriber's acceptance of the update, the cellular telephone 110 transmits a SMS message to the update server processor 100, wherein the message contains an acceptance code and the telephone number of the cellular telephone 110" (see page 5, lines 15-18-emphasis added).

In the Advisory Action mailed 04/11/2006, the Examiner, in response, argued that "[a]pplicant concedes that Lahti teaches a register that contains record of all the subscribers to the anti-virus service, therefore it is inherent or obvious to one of ordinary skill in the art that there is teaching and/or suggestion of registration of the subscribers in order for the center to have the records of the subscribers that subscribe to the service." Appellant respectfully disagrees with the Examiner's inherency/obviousness argument. Whether or not the above statement by the Examiner is correct or not, the Examiner has still not taken into consideration the full weight of appellant's claims. Specifically, Lahti only suggests "registered subscribers" (emphasis added). Merely maintaining a record of registered subscribers simply does not meet a technique "wherein said **mobile data processing device** registers **with a base station** of said wireless telephony network **when said link is established**..." (emphasis added), as claimed by appellant.

Still with respect to independent Claims 1, 10, 19, 28, 37, and 46, the Examiner has relied on paragraphs [0022]-[0027] in Lahti to make a prior art showing of appellant's claimed technique "wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at

least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware."

Appellant respectfully asserts that such excerpt from Lahti only discloses an "SMS request...containing signatures for viruses discovered and analysed since the previous update...which causes the new signature(s) to be incorporated into the anti-virus database for future use." Thus, Lahti teaches that the message only contains the updated virus signatures, and not that the "file includes... at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware," as claimed by appellant. To further emphasize such distinction, appellant points out paragraph [0027] in Lahti which states that "the user is warned 30 and given the opportunity to delete or clean that file." Clearly, a user that must decide whether to delete or clean a file does not suggest that a malware definition updating file "includes at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware" (emphasis added), as appellant claims.

In the Advisory mailed 04/11/2006, the Examiner, in response, argued that "[i]n response to Applicant's argument that Lahti only discloses messages that contain updates and not files, [the] Examiner asserts that Lahti discloses and suggests several ways of obtaining updates..." However, appellant respectfully asserts that the cited excerpts from Lahti fail to even suggest a technique "... where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware" (emphasis added), as claimed. Lahti's teaching that "the user is warned 30 and given the opportunity to delete or clean that file" in no way even suggests that the "definition updating file" itself includes "at least one of a removal action and a disinfection action" (emphasis added), as claimed by appellant. Only appellant teaches and claims an updating file including such specifically claimed action(s).

Furthermore, with respect to independent Claims 1, 10, 19, 28, 37, and 46, the Examiner has failed to specifically address appellant's claimed technique "wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data

processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device" (emphasis added).

Appellant notes, however, that in Lahti "an SMS message [is sent] to the server 12 from a device 1...containing details of which virus signatures are currently stored in the device's signature database" such that "the anti-virus server 12 needs only to issue an SMS request...containing virus signatures not currently on the signature database of the mobile device 1." Thus, Lahti only teaches determining appropriate updated signatures based on signatures already located on the device, and not that a "database includes a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device" (emphasis added), as appellant claims.

In the Advisory mailed 04/11/2006, the Examiner, in response, argued "[i]n response to Applicant's argument that Lahti does not disclose a database that includes a type of mobile device, this limitation is already addressed by [the] Examiner as cited in paragraphs 23-26, the server generates a corresponding update upon request from the subscriber." However, Lahti's disclosure that "[u]pon receipt of a request, the SMS centre 5 generates a corresponding SMS message and send[s] this to the destination mobile device..." simply fails to meet a technique "where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device" (emphasis added), as specifically claimed by appellant. There simply is no disclosure in the excerpts from Lahti relied upon by the Examiner for a technique where "only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device" (emphasis added), as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge

generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computer program product embodied on a computer readable medium for controlling a mobile data processing device to update malware definition data for a malware scanner of said mobile data processing device, said computer program product comprising:

(i) link establishing code operable to establish a wireless telephony link between said mobile data processing device and a public wireless telephony network;

(ii) update receiving code operable to receive malware definition updating data at said mobile data processing device via a data channel of said wireless telephony link; and

(iii) malware definition updating code operable to update malware definition data stored upon said mobile data processing device using said malware definition updating data;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update said malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection

fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

2. (Original) A computer program product as claimed in claim 1, wherein said mobile data processing device is a mobile telephone.

3. (Original) A computer program product as claimed in claim 1, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

4. (Cancelled)

5. (Original) A computer program product as claimed in claim 1, wherein said public wireless telephone network is one of a CDMA network and a GSM network.

6. (Original) A computer program product as claimed in claim 1, wherein said data channel is also used for passing text messages.

7. (Original) A computer program product as claimed in claim 6, wherein said text messages are SMS messages.

8. (Previously Presented) A computer program product as claimed in claim 1, wherein said step of receiving malware definition updating data is initiated from a source of said malware definition updating data.

9. (Original) A computer program product as claimed in claim 1, wherein said data channel

is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

10. (Previously Presented) A computer program product embodied on a computer readable medium for controlling a computer to initiate updating of malware definition data for a malware scanner of a mobile data processing device, said computer program product comprising:

(i) link establishing code operable to establish a wireless telephony link to said mobile data processing device via a public wireless telephony network; and

(ii) update sending code operable to send malware definition updating data to said mobile data processing device via a data channel of said wireless telephony link;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only

malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

11. (Original) A computer program product as claimed in claim 10, wherein said mobile data processing device is a mobile telephone.

12. (Original) A computer program product as claimed in claim 10, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

13. (Cancelled)

14. (Original) A computer program product as claimed in claim 10, wherein said public wireless telephone network is one of a CDMA network and a GSM network.

15. (Original) A computer program product as claimed in claim 10, wherein said data channel is also used for passing text messages.

16. (Original) A computer program product as claimed in claim 15, wherein said text messages are SMS messages.

17. (Original) A computer program product as claimed in claim 10, wherein transfer of malware definition updating data is initiated from a source of said malware definition updating data.

18. (Original) A computer program product as claimed in claim 10, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

19. (Previously Presented) A method of updating malware definition data for a malware scanner of a mobile data processing device, said method comprising the steps of:

(i) establishing a wireless telephony link between said mobile data processing device and a public wireless telephony network;

(ii) receiving malware definition updating data at said mobile data processing device via a data channel of said wireless telephony link; and

(iii) updating malware definition data stored upon said mobile data processing device using said malware definition updating data;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update said malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

20. (Original) A method as claimed in claim 19, wherein said mobile data processing device

is a mobile telephone.

21. (Original) A method as claimed in claim 19, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

22. (Cancelled)

23. (Original) A method as claimed in claim 19, wherein said public wireless telephone network is one of a CDMA network and a GSM network.

24. (Original) A method as claimed in claim 19, wherein said data channel is also used for passing text messages.

25. (Original) A method as claimed in claim 24, wherein said text messages are SMS messages.

26. (Original) A method as claimed in claim 19, wherein transfer of said malware definition updating data is initiated from a source of said malware definition updating data.

27. (Original) A method as claimed in claim 19, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

28. (Previously Presented) A method of updating malware definition data for a malware scanner of a mobile data processing device, said method comprising the steps of:

(i) establishing a wireless telephony link to said mobile data processing device via a public wireless telephony network; and

(ii) sending malware definition updating data to said mobile data processing device via a data channel of said wireless telephony link;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless

telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

29. (Original) A method as claimed in claim 28, wherein said mobile data processing device is a mobile telephone.

30. (Original) A method as claimed in claim 28, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

31. (Cancelled)

32. (Original) A method as claimed in claim 28, wherein said public wireless telephone

network is one of a CDMA network and a GSM network.

33. (Original) A method as claimed in claim 28, wherein said data channel is also used for passing text messages.

34. (Original) A method as claimed in claim 33, wherein said text messages are SMS messages.

35. (Original) A method as claimed in claim 28, wherein transfer of said malware definition updating data is initiated from a source of said malware definition updating data.

36. (Original) A method as claimed in claim 2, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

37. (Previously Presented) Apparatus for controlling a mobile data processing device to update malware definition data for a malware scanner of said mobile data processing device, said apparatus comprising:

(i) link establishing logic operable to establish a wireless telephony link between said mobile data processing device and a public wireless telephony network;

(ii) update receiving logic operable to receive malware definition updating data at said mobile data processing device via a data channel of said wireless telephony link; and

(iii) malware definition updating logic operable to update malware definition data stored upon said mobile data processing device using said malware definition updating data;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update said malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;

wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

38. (Original) Apparatus as claimed in claim 37, wherein said mobile data processing device is a mobile telephone.

39. (Original) Apparatus as claimed in claim 37, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

40. (Cancelled)

41. (Original) Apparatus as claimed in claim 37, wherein said public wireless telephone network is one of a CDMA network and a GSM network.

42. (Original) Apparatus as claimed in claim 37, wherein said data channel is also used for passing text messages.

43. (Original) Apparatus as claimed in claim 42, wherein said text messages are SMS

messages.

44. (Original) Apparatus as claimed in claim 37, wherein said step of transferring is initiated from a source of said malware definition updating data.

45. (Original) Apparatus as claimed in claim 37, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

46. (Previously Presented) Apparatus for controlling a computer to initiate updating of malware definition data for a malware scanner of a mobile data processing device, said apparatus comprising:

(i) link establishing logic operable to establish a wireless telephony link to said mobile data processing device via a public wireless telephony network; and

(ii) update sending logic operable to send malware definition updating data to said mobile data processing device via a data channel of said wireless telephony link;

wherein said mobile data processing device registers with a base station of said wireless telephony network when said link is established such that said base station and said wireless telephony network are notified of a telephone number of said mobile data processing device for use in sending said malware definition updating data to said mobile data processing device;

wherein when received data is received at said mobile data processing device, a type of said received data is identified to determine if said received data is said malware definition updating data, such that if said received data is said malware definition updating data, a digital signature associated with said malware definition updating data is verified;

wherein if said digital signature is not verified, said malware definition updating data is ignored;

wherein if said digital signature is verified, said malware definition updating data is utilized to update malware definition data stored upon said mobile data processing device by appending said malware definition updating data to said malware definition data;

wherein said malware definition updating data is provided in a malware definition updating file, where said file is generated by one of automatically, semi-automatically, and manually upon an analysis of newly discovered malware and where said file includes a detection

fingerprint, and at least one of a removal action and a disinfection action to be taken in response to a detection of said newly discovered malware;
wherein said mobile data processing device is identified by a database of subscribers to an update service associated with said malware scanner, where said database includes said telephone number of said mobile data processing device to which said malware definition updating data is to be sent and a type of said mobile data processing device such that only malware definition updating data that is appropriate to said type of said mobile data processing device is sent to said mobile data processing device.

47. (Original) Apparatus as claimed in claim 46, wherein said mobile data processing device is a mobile telephone.

48. (Original) Apparatus as claimed in claim 46, wherein said mobile data processing device is a personal digital assistant having a connection to said wireless public telephony network.

49. (Cancelled)

50. (Original) Apparatus as claimed in claim 46, wherein said public wireless telephone network is one of a CDMA network and a GSM network.

51. (Original) Apparatus as claimed in claim 46, wherein said data channel is also used for passing text messages.

52. (Original) Apparatus as claimed in claim 51, wherein said text messages are SMS messages.

53. (Original) Apparatus as claimed in claim 46, wherein transfer of malware definition updating data is initiated from a source of said malware definition updating data.

54. (Original) Apparatus as claimed in claim 46, wherein said data channel is open whenever said mobile data processing device is switched on and connected to said public wireless telephony network.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

There is no such related proceeding.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P449/01.143.01).

Respectfully submitted,

By: _____ Date: 10/20/06

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660